

MODULAR FORMS AND ℓ -ADIC REPRESENTATIONS

Séminaire Bourbaki, 21st year, 1968/69, no. 355

February 1969

Pierre Deligne

Editorial note. The controlling source for this English edition is an English retype dated 28 June 2004. The published French Bourbaki original, pp. 139–172, controls the French edition and adjudicates damaged English-retype passages. Evident non-mathematical typographical slips are regularized in the running text; substantive or non-obvious restorations are disclosed in place and registered in the source-alignment ledger delivered with this edition.

1 Introduction

Let

$$D(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n \quad (|q| < 1)$$

and

$$\Delta(z) = D(e^{2\pi iz}) \quad (\operatorname{Im} z > 0).$$

It is known that the function Δ is, up to a constant factor, the unique cusp form of weight 12 for the group $\operatorname{SL}_2(\mathbb{Z})$. Put, for p prime,

$$H_p(X) = 1 - \tau(p)X + p^{11}X^2.$$

Following Hecke's theory, the Dirichlet series

$$L_{\tau}(s) = \sum \tau(n)n^{-s} = \prod_p \frac{1}{H_p(p^{-s})}$$

extends to an entire function of s , and the function

$$(2\pi)^{-s}\Gamma(s)L_{\tau}(s)$$

is invariant under $s \mapsto 12 - s$. Ramanujan's conjecture asserts that the roots of the polynomial H_p have absolute value $p^{-11/2}$; equivalently, $|\tau(p)| < 2p^{11/2}$.

These properties, proven or conjectural, are similar to conjectural properties of zeta functions of algebraic varieties over $\mathbb{Q}$. Suggested by this, as a first approximation, one is tempted to interpret L_{τ} as the zeta function of such a variety.

For each prime number ℓ , let K_{ℓ} be the maximal extension of $\mathbb{Q}$ unramified away from ℓ and, for $p \neq \ell$, let F_p be the inverse in $\operatorname{Gal}(K_{\ell}/\mathbb{Q})$ of the Frobenius element φ_p relative to p . This object is well defined up to conjugation.

Translating the preceding in terms of ℓ -adic cohomology, Serre conjectured the existence, for each ℓ , of a representation of $\operatorname{Gal}(K_{\ell}/\mathbb{Q})$ in a $\mathbb{Q}_{\ell}$ -vector space W_{ℓ} of rank 2 such that, for each $p \neq \ell$,

$$H_p(X) = \det(1 - F_p X; W_{\ell}).$$

Moreover, the representation W_{ℓ} should lie in the range of application of the Weil conjectures, and Ramanujan's conjecture should be a particular case of them.

This program has been carried out by Kuga–Shimura [4] in the analogous case of modular forms relative to certain subgroups of $\operatorname{SL}_2(\mathbb{R})$ with compact quotient. Reduced to the present case, the fundamental idea of Sato–Kuga–Shimura is the following: if E is the universal elliptic curve over the moduli scheme S of elliptic curves (forgetting that it does not exist) and if E^k is the fiber product of E with itself over S , repeated k times, then $L_{\tau}(s)$ is essentially the zeta function of E^k for $k = 10 = 12 - 2$.

We show below how to resolve the difficulties created by the points at infinity, and how to construct the representations W_{ℓ} having the properties indicated above. For more historical details and for applications, see Serre [6].

Source note. The retyped source has “the difficulties creeted by the points.” The evident spelling is regularized, and “at infinity” is restored from the subject of the construction that follows.

Notation.

- We denote by $\mathbb{A}$ the ring of adeles of $\mathbb{Q}$, by $\mathbb{A}_f$ the ring of finite adeles, the restricted product over all prime numbers of the fields $\mathbb{Q}_p$, and, for S a finite set of prime numbers, put

$$\mathbb{A}_f^S = \prod_{p \in S} \mathbb{Q}_p \times \prod_{p \notin S} \mathbb{Z}_p \subset \mathbb{A}_f.$$

Source note. In the second product the retyped source prints $\mathbb{Q}_p$. The restricted-product definition and the immediately following identity $\widehat{\mathbb{Z}} = \mathbb{A}_f^\emptyset$ require $\mathbb{Z}_p$, as delivered here. For $S = \emptyset$, one writes $\widehat{\mathbb{Z}} = \mathbb{A}_f^\emptyset$.

- If X is a topological space, or the étale site of a scheme, and G is a set, G also denotes the constant sheaf on X defined by G .
- We denote by $\mathbb{G}_a$ and $\mathbb{G}_m$ the additive and multiplicative groups.
- An elliptic curve is an abelian variety of dimension one, and in particular is equipped with an origin.
- If L is an invertible sheaf and $n \in \mathbb{Z}$, L^n denotes the n th tensor power $L^{\otimes n}$.
- We denote by $\overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.
- The symbol $\square$ marks the end of a proof, or its absence.

2 The Shimura Isomorphism

(2.1) An elliptic curve over a complex analytic space S is a proper and flat morphism of analytic spaces $f : E \rightarrow S$, equipped with a section e , whose fibers are elliptic curves. An elliptic curve over S admits one and only one S -group law

$$\mu : E \times_S E \rightarrow E$$

whose unit section is e . Associated with an elliptic curve are the following.

- (a) The invertible sheaf

$$\omega_E = e^* \Omega_{E/S}^1.$$

The relative Lie algebra $\text{Lie}_S(E)$ is the invertible sheaf ω^{-1} dual to ω . One has

$$f_* \Omega_{E/S}^1 \xrightarrow{\sim} \omega.$$

- (b) The local system of free rank-2 $\mathbb{Z}$ -modules $R^1 f_* \mathbb{Z}$. One puts

$$T_{\mathbb{Z}}(E) = (R^1 f_* \mathbb{Z})^\vee, \quad T_{\mathbb{Q}}(E) = T_{\mathbb{Z}}(E) \otimes \mathbb{Q},$$

the local system of homology of E over S .

The exponential mapping defines an exact sequence of sheaves of sections

$$0 \longrightarrow T_{\mathbb{Z}}(E) \xrightarrow{\alpha} \omega^{-1} \longrightarrow E \longrightarrow 0,$$

so that the elliptic curve E can be reconstructed from the map α .

The local system $\bigwedge^2 R^1 f_* \mathbb{Z} \simeq R^2 f_* \mathbb{Z}$ is canonically isomorphic to $\mathbb{Z}$. An isomorphism between $\mathbb{Z}^2$ and $R^1 f_* \mathbb{Z}$ is said to be admissible if it induces 1 on second exterior powers. Denote by $\text{Hom}^+(\mathbb{R}^2, \mathbb{C})$ the set of $\mathbb{R}$ -vector-space isomorphisms between $\mathbb{R}^2$ and $\mathbb{C}$ which respect the natural orientations of $\mathbb{R}^2$ and $\mathbb{C}$, defined by $e_1 \wedge e_2 > 0$ and $1 \wedge i > 0$. Such a homomorphism is determined by its restriction to $\mathbb{Z}^2$, and one puts

$$\text{Hom}^+(\mathbb{Z}^2, \mathbb{C}) = \text{Hom}^+(\mathbb{R}^2, \mathbb{C}).$$

Source note. The French original prints that an admissible isomorphism “induces -1 (sic)” and that the elements of Hom^+ “do not respect (sic)” the orientations. The plus sign, the displayed orientations, the Poincaré half-plane in 2.2(ii), and the ensuing construction require respectively 1 and “respect,” as delivered here. This space is equipped with the complex structure obtained from its inclusion in the complex vector space $\text{Hom}(\mathbb{Z}^2, \mathbb{C})$. Over this space one arranges a “universal” exact sequence

$$0 \longrightarrow \mathbb{Z}^2 \xrightarrow{\alpha} \mathbb{G}_a \longrightarrow E_0 \longrightarrow 0.$$

Proposition (2.2).

- (i) The functor which associates with each analytic space S the set of isomorphism classes of elliptic curves E over S , equipped with isomorphisms

$$\omega_E \simeq \mathbb{G}_a, \quad R^1 f_* \mathbb{Z} \simeq \mathbb{Z}^2$$

(the last being admissible), is represented by the analytic space $\mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C})$, equipped with a universal elliptic curve E_0 .

- (ii) The functor which associates with each analytic space S the set of isomorphism classes of elliptic curves over S , equipped with an admissible isomorphism $R^1 f_* \mathbb{Z} \simeq \mathbb{Z}^2$, is represented by the analytic space

$$X = \mathbb{C}^\times \setminus \mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C}),$$

the Poincaré half-plane.

- (iii) The space $\mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C})$ is a principal homogeneous space of the group $\mathbb{G}_m$ over X .

One can again regard X as the set of complex structures on $\mathbb{R}^2$. This space is, by (ii), equipped with a universal elliptic curve E_X , whose local system of real cohomology is canonically isomorphic to $\mathbb{R}^2$. Let ω be the invertible sheaf associated with E_X .

The coherent analytic sheaf

$$R^1 f_* \mathbb{R} \otimes_{\mathbb{R}} \mathcal{O}_X$$

is the relative de Rham cohomology sheaf of E_X over X , and as such it is inserted into an exact sequence, the Hodge filtration,

$$0 \longrightarrow \omega \longrightarrow R^1 f_* \mathbb{R} \otimes_{\mathbb{R}} \mathcal{O}_X \xrightarrow{q} \omega^{-1} \longrightarrow 0$$

since, by Serre duality, $\omega^{-1} \simeq R^1 f_* \mathcal{O}_{E_X}$.

The functorial description in 2.2(ii) evidently gives a right action of the group $\mathrm{SL}_2(\mathbb{Z})$ on (X, E_X) : to $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and to the elliptic curve E equipped with $\alpha : \mathbb{Z}^2 \xrightarrow{\sim} R^1 f_* \mathbb{Z}$, one associates $(E, \alpha \circ \gamma)$. If one regards X , equipped with

$$q : \mathbb{R}^2 \otimes_{\mathbb{R}} \mathcal{O}_X \simeq R^1 f_* \mathbb{R} \otimes_{\mathbb{R}} \mathcal{O}_X \longrightarrow \omega^{-1},$$

as classifying the complex structures on $\mathbb{R}^2$, one has the same evident action of the group $\mathrm{GL}_2^+(\mathbb{R})$ on $(X, \mathbb{R}^2, \omega, q)$.

(2.3) Choose a basis (x_1, x_2) of $\mathbb{R}^2$ such that $x_1 \wedge x_2 > 0$. A point

$$(f : \mathbb{R}^2 \rightarrow \mathbb{C}) \quad \text{mod } \mathbb{C}^\times$$

of X is located by

$$z = \frac{f(x_1)}{f(x_2)} \quad (\mathrm{Im} z > 0),$$

and the map q is identified with

$$q : \mathbb{R}^2 \rightarrow \mathbb{G}_a, \quad ax_1 + bx_2 \longmapsto az + b.$$

This gives an evident trivialization of ω^{-1} over X , which is not equivariant. Relative to this trivialization, a section $f(z)$ of ω^k over X is transformed by an element

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in \mathrm{GL}^+(\mathbb{R}^2)$$

(with respect to the basis (x_1, x_2)) by

$$f \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} (z) = (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right).$$

Source note. In the first matrix on the printed line, both the French original and the English retype have $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1}$. The fractional-linear formula on that same line and the determinant matrix immediately below both require $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$, as delivered here. From the identity

$$dz = (cz + d)^2 d\left(\frac{az + b}{cz + d}\right) \left| \begin{matrix} a & b \\ c & d \end{matrix} \right|^{-1},$$

one deduces that dz is a section of $\omega^{-2} \Omega_X^1$ invariant under $\mathrm{SL}_2(\mathbb{R})$. This section is everywhere nonzero and defines an equivariant isomorphism of $\mathrm{SL}_2(\mathbb{R})$ -sheaves between ω^2 and Ω_X^1 .

(2.4) Let Γ be a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ which has no elements of finite order and has quotient of finite volume. One then knows that the quotient space X/Γ is identified with a smooth projective curve $\overline{X/\Gamma}$ minus a finite number of points. The group Γ acts on X without fixed points. The equivariant local system $\mathbb{R}^2$ on X , as well as the exact sequence

$$0 \rightarrow \omega \rightarrow \mathbb{R}^2 \otimes_{\mathbb{R}} \mathcal{O} \rightarrow \omega^{-1} \rightarrow 0,$$

therefore define a local system U over X/Γ and an exact sequence

$$0 \rightarrow \omega \rightarrow U \otimes_{\mathbb{R}} \mathcal{O} \rightarrow \omega^{-1} \rightarrow 0. \quad (2.5)$$

In the particular case where $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, these structures are obtained from an elliptic curve E over X/Γ whose inverse image is the equivariant elliptic curve E_X over X .

(2.6) The points at infinity of X/Γ are described as follows (see [9]).

- (a) They correspond to conjugacy classes in Γ of nontrivial subgroups of Γ which are maximal among the subgroups of Γ consisting of unipotent elements.
- (b) Let $\Gamma_0 \subset \Gamma$ be one such subgroup and choose a basis (x_1, x_2) of $\mathbb{R}^2$ such that, in this basis, Γ_0 is represented as the set of matrices

$$\left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}.$$

Let z be the coordinate (2.3) on X defined by (x_1, x_2) . There exists N such that the subset

$$X_N = \{z \mid \mathrm{Im} z > N\}$$

of X is disjoint from all of its conjugates γX_N for $\gamma \in \Gamma/\Gamma_0$, so that $X_N/\Gamma_0 \hookrightarrow X/\Gamma$. The function $q = e^{2\pi iz}$ establishes an isomorphism between X_N/Γ_0 and the punctured disk

$$0 < |q| < e^{-2\pi N}.$$

If P_{Γ_0} is the point of $\overline{X/\Gamma} - X/\Gamma$ associated with Γ_0 , this isomorphism extends to an isomorphism of a neighborhood of P_{Γ_0} with the disk $0 \leq |q| < e^{-2\pi N}$.

Source note. The retyped source prints the two disk inequalities without absolute-value bars around the complex coordinate q . The disk description requires $|q|$, which is restored in both inequalities above.

By virtue of (2.3), the sections of ω over X_N which are invariant under Γ_0 are identified with periodic holomorphic functions of period one on X_N . One again denotes by ω the invertible sheaf over $\overline{X/\Gamma}$ which extends ω and such that, in a neighborhood of a point P_{Γ_0} , the section of ω over X_N/Γ_0 defined by the function 1 extends to an invertible section on X_N/Γ_0 .

(2.7) Over X/Γ one has the two invertible sheaves Ω^1 and ω^2 , and an isomorphism φ (2.3) between their restrictions to X/Γ . From the formula

$$dq = d(e^{2\pi iz}) = 2\pi i e^{2\pi iz} dz = 2\pi i q dz$$

it follows that the map

$$\varphi : \Omega^1 \rightarrow \omega^2$$

extends to $\overline{X/\Gamma}$, and has a simple zero at each of the points at infinity.

Definition (2.8). *The space of cusp forms of weight $k+2$, relative to the group Γ , is the space of global sections*

$$H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k).$$

By virtue of (2.7), this space is again identified with the space of global sections of ω^{k+2} vanishing at infinity, that is, at each “point.”

(2.9) Denote by U^k the k th symmetric power of the local system U over X/Γ . The map (2.5) induces a map

$$\iota^k : \omega^k \rightarrow U^k \otimes_{\mathbb{R}} \mathcal{O},$$

hence a map, again denoted by ι^k ,

$$\iota^k : \Omega^1 \otimes \omega^k \rightarrow \Omega^1(U^k),$$

where the target is the sheaf of holomorphic differential forms over X/Γ with coefficients in the local system U^k .

The de Rham resolution of $U^k \otimes_{\mathbb{R}} \mathbb{C}$,

$$0 \rightarrow U^k \otimes_{\mathbb{R}} \mathbb{C} \rightarrow U^k \otimes_{\mathbb{R}} \mathcal{O} \xrightarrow{d} U^k \otimes_{\mathbb{R}} \Omega^1 \rightarrow 0,$$

induces a map

$$\delta : H^0(X/\Gamma, \Omega^1(U^k)) \rightarrow H^1(X/\Gamma, U^k \otimes \mathbb{C}).$$

Moreover, the cohomology space $H^1(X/\Gamma, U^k \otimes \mathbb{C})$ is equipped with a natural complex conjugation, such that δ defines a conjugate-linear mapping $\bar{\delta}$ from the complex conjugate of $H^0(X/\Gamma, \Omega^1(U^k))$ into $H^1(X/\Gamma, U^k \otimes \mathbb{C})$. One thus obtains a map

$$\begin{aligned} \text{sh}_0 &= \delta \circ H^0(\iota^k) \oplus \bar{\delta} \circ H^0(\bar{\iota}^k) \\ \text{sh}_0 : H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k)} &\longrightarrow H^1(X/\Gamma, U^k \otimes \mathbb{C}). \end{aligned}$$

For an arbitrary sheaf F on a space Y , one denotes by $\tilde{H}^i(Y, F)$ the image of cohomology with compact supports $H_c^i(Y, F)$ in cohomology without supports $H^i(Y, F)$.

Theorem 4.2.6 of [9] is essentially equivalent to the following theorem; in loc. cit. k is supposed even, but the same proof works in general.

Theorem (2.10, Shimura [7]). *There exists an isomorphism sh making the following diagram commutative:*

$$\begin{array}{ccc} H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k)} & \xrightarrow{\text{sh}} & \tilde{H}^1(X/\Gamma, U^k \otimes \mathbb{C}) \\ \cap & & \cap \\ H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k)} & \xrightarrow{\text{sh}_0} & H^1(X/\Gamma, U^k \otimes \mathbb{C}). \end{array}$$

One calls sh the Shimura isomorphism.

(2.11) In the particular case where Γ is a subgroup of finite index of $\text{SL}_2(\mathbb{Z})$, the elliptic curve E over X/Γ furnishes an elliptic curve scheme over the algebraic curve $\overline{X/\Gamma}$; equivalently, its modular invariant is meromorphic at infinity. It therefore admits a Néron model $\bar{E}$ over $\overline{X/\Gamma}$. One can show that the fibers of $\bar{E}$ at the points at infinity are of multiplicative type, and that over all of $\overline{X/\Gamma}$ one has

$$\omega = e^* \Omega_{\bar{E}/\overline{X/\Gamma}}^1.$$

In this particular case, one has $U = R^1 f_* \mathbb{Z} \otimes \mathbb{R}$, so that the target of the Shimura isomorphism can be rewritten as

$$\tilde{H}^1(X/\Gamma, U^k \otimes \mathbb{C}) \simeq \tilde{H}^1(X/\Gamma, \text{Sym}^k(R^1 f_* \mathbb{Z})) \otimes_{\mathbb{Z}} \mathbb{C}.$$

Source note. The printed text twice has the typographical form “fournishes”; both occurrences are delivered as “furnishes.”

3 Hecke Operators and the Fundamental ℓ -adic Representation

(3.1) Recall (cf. [3]) that the category of “locally constant” constructible $\mathbb{Z}_{\ell}$ -sheaves, abbreviated lcc, over a scheme S is the category of projective systems $(F_n)_{n \in \mathbb{N}}$ on the étale site $S_{\text{ét}}$ of S satisfying:

- (i) F_n is a locally constant sheaf of $\mathbb{Z}/(\ell^n)$ -modules of finite type;
- (ii) if $n \leq m$, then

$$F_m \otimes_{\mathbb{Z}/(\ell^m)} \mathbb{Z}/(\ell^n) \xrightarrow{\sim} F_n.$$

The lcc $\mathbb{Z}_\ell$ -sheaves form a stack of abelian categories over S ; the stack of lcc $\mathbb{Q}_\ell$ -sheaves is the quotient of this stack by the thick substack of lcc $\mathbb{Z}_\ell$ -sheaves killed by a power of ℓ . One denotes by $\otimes_{\mathbb{Q}_\ell}$ the canonical functor from the category of lcc $\mathbb{Z}_\ell$ -sheaves into that of lcc $\mathbb{Q}_\ell$ -sheaves.

If S is connected and equipped with a geometric point s , the category of lcc $\mathbb{Z}_\ell$ -sheaves, respectively $\mathbb{Q}_\ell$ -sheaves, over S is equivalent, by the functor “fiber over s ,” to the category of continuous representations of the fundamental group $\pi_1(S, s)$ on $\mathbb{Z}_\ell$ -modules of finite type, respectively on finite-dimensional $\mathbb{Q}_\ell$ -vector spaces.

If T is a finite set of prime numbers, an lcc $\mathbb{A}_T^f$ -sheaf consists of the giving, for each prime number ℓ , of an lcc $\mathbb{Z}_\ell$ -sheaf if $\ell \notin T$, and an lcc $\mathbb{Q}_\ell$ -sheaf if $\ell \in T$. For $T = \emptyset$, one speaks of lcc $\widehat{\mathbb{Z}}$ -sheaves rather than of lcc $\mathbb{A}_\emptyset^f$ -sheaves.

For general T , the category of lcc $\mathbb{A}_T^f$ -sheaves is the inductive limit of the categories of lcc $\mathbb{A}_{T'}^f$ -sheaves for $T' \subset T$ finite. One puts

$$\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/(\ell^n), \quad \mathbb{Q}_\ell = \mathbb{Z}_\ell \otimes \mathbb{Q}, \quad \widehat{\mathbb{Z}} = (\mathbb{Z}_\ell)_\ell, \quad \mathbb{A}_T^f = \widehat{\mathbb{Z}} \otimes \mathbb{A}_T^f.$$

Source note. The English retype’s obvious spelling slips on this page—including “Shiumra,” “particular,” “schme,” “constant,” and “numbesr”—are regularized without changing their mathematical content.

The stack of elliptic curves up to isogeny over S is the stack obtained from the stack of elliptic curves over S by “formally inverting isogenies.” One denotes by $\otimes_{\mathbb{Q}}$ the functor associating to an elliptic curve its underlying elliptic curve up to isogeny. For S quasi-compact, one has

$$\mathrm{Hom}(E, F) \otimes \mathbb{Q} \xrightarrow{\sim} \mathrm{Hom}(E \otimes \mathbb{Q}, F \otimes \mathbb{Q}),$$

and, for S normal, every elliptic curve up to isogeny over S underlies an elliptic curve over S .

(3.2) Let $f : E \rightarrow S$ be an elliptic curve over a scheme S . One denotes by $T_\ell(E)$ the projective system of kernels E_{ℓ^n} of multiplication by ℓ^n on E , the transition maps from E_{ℓ^n} to E_{ℓ^m} , for $n \geq m$, being multiplication by ℓ^{n-m} . Proceeding in the same way for $\mathbb{G}_m$, one puts $T_\ell(\mathbb{G}_m) = \mathbb{Z}_\ell(1)$. If ℓ is invertible on S , then $T_\ell(E)$ and $\mathbb{Z}_\ell(1)$ are $\mathbb{Z}_\ell$ -sheaves on S . One defines $T_\infty(E)$ to be the relative Lie algebra of E over S , that is, the invertible dual of the invertible sheaf ω of (2.1(a)).

Suppose S is of characteristic 0. One then defines the $\widehat{\mathbb{Z}}$ -sheaf $T_f(E)$ over S to be the system of the $T_\ell(E)$, and puts

$$V_f(E) = T_f(E) \otimes \mathbb{A}_f.$$

If $u : E \rightarrow F$ is an isogeny, then u induces an isomorphism of $V_f(E)$ onto $V_f(F)$ and of $T_\infty(E)$ onto $T_\infty(F)$; the functors V_f and T_∞ therefore factor through the category of elliptic curves up to isogeny over S .

Proposition (3.3). *Let S be a scheme of characteristic 0; let $E_1(S)$ be the category of elliptic curves over S ; and let $E_2(S)$ be the category of triples composed of an elliptic curve up to isogeny E over S , a $\widehat{\mathbb{Z}}$ -sheaf T which is a twisted form of $\widehat{\mathbb{Z}}^2$, and an isomorphism*

$$\beta : V_f(E) \xrightarrow{\sim} T \otimes \mathbb{A}_f.$$

Then the functor

$$I : E \longmapsto (E \otimes \mathbb{Q}, T_f(E), V_f(E) \simeq T_f(E) \otimes \mathbb{A}_f)$$

from $E_1(S)$ to $E_2(S)$ is an equivalence of categories.

The question is local on S , which one may suppose quasi-compact. If $f : E \rightarrow F$ is a morphism of S -elliptic curves, and if f is an isogeny, then one has an exact sequence

$$0 \rightarrow T_f(E) \rightarrow T_f(F) \rightarrow \ker(f) \rightarrow 0. \quad (3.4)$$

The morphism f is divisible by n if and only if it kills the kernel E_n of multiplication by n , because the “multiplication by n ” map $E/E_n \rightarrow E$ is an isomorphism. By (3.4), this holds if and only if $T_f(f)$ is divisible by n , and one deduces from this that $\mathrm{Hom}_S(E, F)$ is the subgroup of $\mathrm{Hom}_S(E \otimes \mathbb{Q}, F \otimes \mathbb{Q})$ consisting of the morphisms f such that $V_f(f)$ sends $T_f(E)$ into $T_f(F)$. The functor I is thus fully faithful.

Source note. The canonical French original says “pleinement fidèle,” whereas the inherited English retype says “faithfully flat.” Since I is a functor between categories and the preceding argument identifies its Hom sets, the

French reading “fully faithful” is retained. The English retype’s obvious case slips $u : e \rightarrow F$ and $E_1(s)$ are normalized to $u : E \rightarrow F$ and $E_1(S)$.

Let $X \in \text{Ob}(E_2(S))$. Locally on S , X is defined by an elliptic curve up to isogeny $E \otimes \mathbb{Q}$, and by a “lattice” T in $V_f(E)$ which, for almost all ℓ , coincides with $T_\ell(E)$. For $q \in \mathbb{Q}$, $(E \otimes \mathbb{Q}, T)$ is isomorphic to $(E \otimes \mathbb{Q}, qT)$, which allows us to suppose that $T_f(E) \subset T$. The quotient $K = T/T_f(E)$ is then canonically isomorphic to a finite subgroup of E , and X is the image of E/K under I (cf. 3.4). $\square$

Corollary (3.5). *The functor $F_1(S)$, respectively $F'_1(S)$, which associates with each scheme S of characteristic 0 the set of isomorphism classes of elliptic curves over S equipped with an isomorphism*

$$\alpha : T_f(E) \xrightarrow{\sim} \widehat{\mathbb{Z}}^2$$

respectively also with an isomorphism

$$\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathbb{G}_a,$$

is isomorphic to the functor $F_2(S)$, respectively $F'_2(S)$, which associates with S the set of isomorphism classes of elliptic curves up to isogeny over S , equipped with an isomorphism

$$\beta : V_f(F) \xrightarrow{\sim} \mathbb{A}_f^2$$

respectively also with an isomorphism

$$\beta_\infty : T_\infty(F) \xrightarrow{\sim} \mathbb{G}_a.$$

Proposition (3.6). *The functor F_1 (respectively F'_1) is represented by a scheme M_∞ (respectively M'_∞) over $\mathbb{Q}$.*

Let $n \geq 3$ be an integer. The functor which associates with each scheme S the set of isomorphism classes of elliptic curves, equipped with an isomorphism

$$\alpha_n : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$$

respectively also with $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$, is represented by an affine curve M_n (respectively by an affine surface M'_n) over $\text{Spec}(\mathbb{Z}[1/n])$. For $n \mid m$, the morphism from M_m to M_n defined by

$$(E, \alpha_m : E_m \xrightarrow{\sim} (\mathbb{Z}/m)^2) \longmapsto (E, (n/m)\alpha_m : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2)$$

is finite and étale over $\text{Spec}(\mathbb{Z}[1/m])$, and one has

$$M_\infty = \varprojlim M_n.$$

One proceeds in the same way to represent F'_1 . $\square$

Source note. The canonical French original gives $\mathcal{O}_S$ and the factor $(n/m)\alpha_m$. The inherited readings $\mathcal{O}_X$ and $(m/n)\alpha_m$, incompatible with the functor’s base and with restriction of level for $n \mid m$, are corrected in both editions. The English retype’s “schem” and duplicated phrase “One goes one proceeds” are also regularized to “scheme” and “One proceeds.”

(3.7) The scheme M_∞ (respectively M'_∞) is equipped with a universal elliptic curve $f_\infty : E_\infty \rightarrow M_\infty$ and an isomorphism

$$\alpha : T_f(E_\infty) \xrightarrow{\sim} \widehat{\mathbb{Z}}^2,$$

respectively also with an isomorphism

$$\alpha_\infty : T_\infty(E_\infty) \xrightarrow{\sim} \mathbb{G}_a.$$

Following (3.5), the scheme M_∞ (respectively M'_∞) represents the functor F_2 (respectively F'_2), which gives an evident left action of the adelic group $\text{GL}_2(\mathbb{A}_f)$ on

$$(M_\infty, E_\infty \otimes \mathbb{Q}, \alpha \otimes \mathbb{A}_f)$$

respectively on

$$(M'_\infty, E_\infty \otimes \mathbb{Q}, \alpha \otimes \mathbb{A}_f, \alpha_\infty).$$

On the functor this action is given, for $g \in \text{GL}_2(\mathbb{A}_f)$, by

$$g : (F, \beta : V_f(F) \xrightarrow{\sim} \mathbb{A}_f^2, \beta_\infty) \longmapsto (F, g \circ \beta : V_f(F) \xrightarrow{\sim} \mathbb{A}_f^2, \beta_\infty).$$

Source note. Both printed witnesses abbreviate the induced trivialization as $\alpha \otimes \mathbb{A}_f^2$ and write $V_f(E)$ inside a tuple whose elliptic curve is F . Since $\alpha : T_f(E_\infty) \rightarrow \widehat{\mathbb{Z}}^2$, scalar extension is $\alpha \otimes \mathbb{A}_f$, and the action's domain is $V_f(F)$; these type-required readings are delivered above. The French original also uses the same universal curve E_∞ in both tuples; the inherited prime on E'_∞ is therefore removed in both editions. Shafarevich first noted this fact.

Let Y be a scheme over $\mathbb{C}$, equal to the projective limit of schemes Y_i of finite type over $\mathbb{C}$, with finite transition maps. The locally compact ringed space Y^{an} , equal to the projective limit of the Y_i^{an} , depends only on Y and not on its representation as a projective limit. If Y is a scheme over $\mathbb{Q}$, equal to the projective limit of schemes Y_i of finite type over $\mathbb{Q}$ with finite transition maps, one puts $Y^{\text{an}} = (Y \otimes \mathbb{C})^{\text{an}}$. This applies to M_∞ and M'_∞ .

Proposition (3.8). *One has canonically*

$$M'^{\text{an}}_\infty \simeq \text{Hom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}_f^2) / \text{GL}_2(\mathbb{Q})$$

and

$$M^{\text{an}}_\infty \simeq \mathbb{C}^\times \backslash \text{Hom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}_f^2) / \text{GL}_2(\mathbb{Q}),$$

and, less canonically,

$$M'^{\text{an}}_\infty \simeq \text{GL}_2(\mathbb{A}) / \text{GL}_2(\mathbb{Q}), \quad M^{\text{an}}_\infty \simeq K_\infty \backslash \text{GL}_2(\mathbb{A}) / \text{GL}_2(\mathbb{Q}),$$

where K_∞ is the maximal compact subgroup at infinity, enlarged by the real homotheties. These isomorphisms are compatible with the action of $\text{GL}_2(\mathbb{A}_f)$.

Source note. The IAS English retype contains unresolved “[a/the, bad copy]” and “[bad copy]” placeholders here. The canonical French original reads exactly that K_∞ is the maximal compact subgroup at infinity, enlarged by the real homotheties; that source-established wording is delivered above.

The notion of elliptic curve up to isogeny, and its variants, extends to the complex analytic case. On the other hand, an isogeny $\varphi : E \rightarrow F$ induces an isomorphism φ^* between the local systems of rational cohomology of E and F , which allows us to define this last object for an elliptic curve up to isogeny. Let S be a complex analytic space. With the aid of (2.1), one sees that to give an elliptic curve up to isogeny over S is equivalent to giving an invertible sheaf T_∞ , a local system $T_\mathbb{Q}$ of $\mathbb{Q}$ -vector spaces, and a morphism $\alpha : T_\mathbb{Q} \rightarrow T_\infty$ inducing an isomorphism $T_\mathbb{Q} \otimes \mathbb{R} \rightarrow T_\infty$ point by point.

Let n be an integer and let K_n be the kernel of the natural mapping

$$\prod_{\ell} \text{GL}_2(\mathbb{Z}_\ell) \rightarrow \text{GL}_2(\mathbb{Z}/n).$$

Let G_1 be the functor which associates with S the set of isomorphism classes of elliptic curves $f : E \rightarrow S$ over S , equipped with an isomorphism

$$\varphi : \mathbb{Q}^2 \xrightarrow{\sim} T_\mathbb{Q}(E),$$

an isomorphism $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$, and an isomorphism $\alpha_n : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$. As in (3.3), one sees that G_1 is isomorphic to the functor G_2 which associates with S the set of isomorphism classes of elliptic curves up to isogeny E over S , equipped with $\varphi : \mathbb{Q}^2 \xrightarrow{\sim} T_\mathbb{Q}(E)$, $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$, and an isomorphism $V_f(E) \xrightarrow{\sim} \mathbb{A}_f^2$ given locally over S up to composition with an element of K_n .

Such an object is determined by the composite map φ' (given locally modulo K_n) obtained from

$$\varphi' : \mathbb{Q}^2 \xrightarrow{\varphi} T_\mathbb{Q}(E) \longrightarrow T_\infty(E) \times V_f(E) \xrightarrow{\sim} \mathcal{O}_S \times \mathbb{A}_f^2.$$

One has

$$E = \mathcal{O}_S / \varphi'(\mathbb{Q}^2 \cap \varphi'^{-1}(T_\infty(E) \times T_f(E))) = \widehat{\mathbb{Z}}^2 \backslash (\mathcal{O}_S \times \mathbb{A}_f^2) / \varphi'(\mathbb{Q}^2),$$

so that, cf. 2.2, G_1 and G_2 are represented by

$$K_n \backslash \text{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}_f^2).$$

Suppose still that $n \geq 3$, so that $\text{GL}_2(\mathbb{Q})$ acts freely on the preceding space. The analytic space M_n^{an} , respectively M'_n , represents the functor analogous in analytic geometry to the functor represented by M_n , respectively M'_n , because this functor, say X , is representable and the arrow $X \rightarrow M_n^{\text{an}}$, respectively $X \rightarrow M'_n$, induces a

bijection on sets of points with values in any finite-rank $\mathbb{C}$ -algebra. Consequently one deduces from the preceding that

$$M_n'^{\text{an}} \simeq K_n \setminus \text{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}_f^2) / \text{GL}_2(\mathbb{Q}).$$

Proceeding in the same way for M_n , one obtains the first assertion of (3.8) by passage to the limit on n .

A point x of

$$\text{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}_f^2) / \text{GL}_2(\mathbb{Q})$$

is identified with a “lattice” L_x of $\mathbb{C} \times \mathbb{A}_f^2$, and the corresponding curve is

$$E_x \simeq \widehat{\mathbb{Z}}^2 \setminus (\mathbb{C} \times \mathbb{A}_f^2) / L_x,$$

equipped with

$$V_f(E_x) \simeq L_x \otimes \mathbb{A}_f \xrightarrow{\sim} \mathbb{A}_f^2.$$

The last assertion of (3.8) follows easily. $\square$

Denote by $f_n : E \rightarrow M_n$ the universal elliptic curve over M_n . The integer k being fixed, one makes the following definition.

Definition (3.9). *One denotes by W (or by ${}^k W$ if confusion is possible) the $\mathbb{Q}$ -vector space*

$$W = \varinjlim_n \widetilde{H}^1(M_n^{\text{an}}, \text{Sym}^k(R^1 f_{n*} \mathbb{Q})) = \varinjlim_n W.$$

Source note. The retype’s page-level slips “beause,” “arros,” and “Once deduces” are regularized. In the description of the curve corresponding to x , the printed $V_f(E)$ is delivered as $V_f(E_x)$, the only object just defined there. The English retype then says that W “doesn’t depend on” the universal curve, reversing the canonical French “ne dépend que de.” The source-coherent reading “depends only on” is delivered below in both editions. The level index n , visible in the French f_{n*} , is also restored in the first formula defining W .

This vector space depends only on the universal elliptic curve, up to isogeny, $f_\infty : E \rightarrow M_\infty$, so that, by transport of structure, it is equipped with a left action of the adelic group $\text{GL}_2(\mathbb{A}_f)$.

If ℓ is a prime number, the vector space $W_\ell = W \otimes \mathbb{Q}_\ell$ admits a purely algebraic definition, in terms of the ℓ -adic cohomology of the scheme over the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ obtained from M_n by extension of scalars:

$$W_\ell = \varinjlim_n \widetilde{H}^1(M_n \otimes \overline{\mathbb{Q}}, \text{Sym}^k(R^1 f_{n*} \mathbb{Q}_\ell)) = \varinjlim_n W_\ell. \quad (3.10)$$

Thus the Galois group of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$ acts, by transport of structure, on W_ℓ and on the finite-level spaces.

Finally, the space M_n^{an} is the disjoint union of quotients of the Poincaré half-plane by congruence subgroups of $\text{SL}_2(\mathbb{Z})$, so that, denoting by ω the invertible sheaf on M_n defined by E , Shimura’s theory (2.10) gives

$$W_\infty = W \otimes \mathbb{C} = \varinjlim_n \left(H^0(\overline{M}_n^{\text{an}}, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(\overline{M}_n^{\text{an}}, \Omega^1 \otimes \omega^k)} \right). \quad (3.11)$$

Source note. The inherited transcription dropped the bars on the compactified curves $\overline{M}_n^{\text{an}}$ in both summands of (3.11); they are restored above. The retype’s opening “if is equipped” is regularized to “it is equipped.” This decomposition of $W \otimes \mathbb{C}$ into two complex-conjugate subspaces, one of which is the space of all cusp forms of weight $k+2$ relative to a general congruence subgroup of $\text{SL}_2(\mathbb{Z})$, is analogous to a Hodge decomposition, of type

$$(0, k+1) + (k+1, 0).$$

The action of the adelic group commutes with the action of the Galois group and respects the preceding decomposition.

While the ℓ -adic local system $R^1 f_* \mathbb{Q}_\ell$ is trivial on M_∞ , I do not know whether there is a relation between W_ℓ and

$$\varinjlim_n (\widetilde{H}^1(M_n \otimes \overline{\mathbb{Q}}, \mathbb{Q}_\ell) \otimes \text{Sym}^k(\mathbb{Q}_\ell^2)).$$

(3.12) Let $n \geq 3$ be an integer and let K_n be as in (3.8). Then one has

$$W^{K_n} = {}_n W.$$

This follows by passage to the limit and from the fact that, in rational cohomology, the cohomology of the quotient of a space by a finite group is obtained by taking the invariants of that group in the cohomology.

Put, for p prime,

$$W^{(p)} = W^{\mathrm{GL}_2(\mathbb{Z}_p)}.$$

By passage to the limit, one obtains

$$W^{(p)} = \varinjlim_{(n,p)=1} {}_n W.$$

On this cohomology space there again act:

- (i) the subgroup $\prod_{\ell \neq p} \mathrm{GL}_2(\mathbb{Q}_\ell)$ of $\mathrm{GL}_2(\mathbb{A}_f)$, because this subgroup centralizes $\mathrm{GL}_2(\mathbb{Z}_p)$;
- (ii) the Hecke algebra $\mathcal{H}(\mathrm{GL}_2(\mathbb{Q}_p), \mathrm{GL}_2(\mathbb{Z}_p))$, which is the algebra of integral measures on the discrete space $\mathrm{GL}_2(\mathbb{Q}_p)/\mathrm{GL}_2(\mathbb{Z}_p)$ invariant on the left by $\mathrm{GL}_2(\mathbb{Z}_p)$. This subalgebra of the group algebra of $\mathrm{GL}_2(\mathbb{Q}_p)$ acts on W and respects $W^{(p)}$. It acts already on each ${}_n W$ for n prime to p .

The Hecke algebra admits as a basis the measures associated with characteristic functions of the double cosets of $\mathrm{GL}_2(\mathbb{Z}_p)$ in $\mathrm{GL}_2(\mathbb{Q}_p)$, and one knows that

$$\mathcal{H}(\mathrm{GL}_2(\mathbb{Q}_p), \mathrm{GL}_2(\mathbb{Z}_p)) = \mathbb{Z}[T_p, R_p, R_p^{-1}],$$

where T_p and R_p are the double cosets of

$$\begin{pmatrix} 1 & 0 \\ 0 & p^{-1} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} p^{-1} & 0 \\ 0 & p^{-1} \end{pmatrix}.$$

(3.13) Let p be a prime number, let $n \geq 3$ be an integer prime to p , and let $F_{n,p}$ be the functor which associates to each scheme S the set of isomorphism classes of commutative diagrams of S -schemes

$$\begin{array}{ccc} & & \mathbb{Z}/(n)^2 \\ & \alpha \nearrow & \nwarrow \alpha' \\ E_n & \longrightarrow & F_n \\ \cap & & \cap \\ E & \xrightarrow{\varphi} & F \end{array} \quad (3.14)$$

where φ is a p -isogeny between elliptic curves and α is an isomorphism. One denotes by q_1 and $q_2 : F_{n,p} \rightarrow M_n$ the morphisms of functors associating to a diagram (3.14) the subdiagrams (E, E_n, α) and (F, F_n, α') .

Proposition (3.15). *The functor $F_{n,p}$ is represented by a scheme $M_{n,p}$, and the morphisms $q_1, q_2 : M_{n,p} \rightarrow M_n$ are finite.*

The automorphism σ of $F_{n,p}$ sending $\varphi : E \rightarrow F$ to ${}^t\varphi : F \rightarrow E$ exchanges q_1 and q_2 ; it suffices therefore to consider q_1 . This morphism identifies $F_{n,p}$ with the functor of subgroups of order p of the universal elliptic curve E over M_n , so that, by the theory of Hilbert schemes, $F_{n,p}$ is representable and $M_{n,p}$ is proper over M_n . If s is a geometric point of M_n , $q_1^{-1}(s)$ is the set of subgroups of order p of E_s , and has $p+1$ elements if $\mathrm{char}(k(s)) \neq p$, and only one, the kernel of Frobenius, if $\mathrm{char}(k(s)) = p$. $\square$

One can show that $M_{n,p}$ is regular, and that q_1 and q_2 are finite flat; we do not use this delicate result, but content ourselves here to note that over $\mathrm{Spec}(\mathbb{Z}[1/p])$, each q_i makes $M_{n,p}$ an étale covering of degree $p+1$ of M_n .

The morphisms q_i can be inserted into a commutative diagram

$$\begin{array}{ccccc} & q_1^* E & \xrightarrow{\varphi} & q_2^* E & \\ & \swarrow & & \searrow & \\ E & & & & E \\ & \searrow & & \swarrow & \\ & M_{n,p} & & & \\ & \swarrow & & \searrow & \\ E & & & & E \\ & \searrow & & \swarrow & \\ & M_n & & & M_n \end{array} \quad (3.16)$$

where (φ, u, v) is part of the universal diagram (3.14).

Source note. In the inherited TeX, diagram (3.16) attached u and v to the lower object $M_{n,p}$ and collapsed the two diagonal pullback maps. The source has $u : q_1^* E \rightarrow M_{n,p}$ and $v : q_2^* E \rightarrow M_{n,p}$, with separate unlabeled diagonal maps from each pullback to E ; the native diagram above restores that topology.

One denotes by I_p the morphism from M_n to M_n corresponding to the morphism of functors $(E, \alpha) \mapsto (E, \alpha/p)$:

$$\begin{array}{ccc} E & \longrightarrow & E \\ \downarrow & & \downarrow \\ M_n & \xrightarrow{I_p} & M_n \end{array} \quad I_p^*(E, \alpha) = (E, \alpha/p). \quad (3.17)$$

I_p^* is an automorphism of $\tilde{H}^i(M_n^{\text{an}}, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}))$. It is tiresome, but routine, to prove the following.

Proposition (3.18).

(i) The endomorphism T_p of ${}_n W$ is expressed, with the aid of (3.16), as the composite map

$$\begin{aligned} \tilde{H}^1(M_n^{\text{an}}, \text{Sym}^k(R^1 f_{n*} \mathbb{Q})) &\xrightarrow{q_2^*} \tilde{H}^1(M_{n,p}^{\text{an}}, \text{Sym}^k(R^1 v_* \mathbb{Q})) \\ &\xrightarrow{\varphi^*} \tilde{H}^1(M_{n,p}^{\text{an}}, \text{Sym}^k(R^1 u_* \mathbb{Q})) \xrightarrow{q_{1*}} \tilde{H}^1(M_n^{\text{an}}, \text{Sym}^k(R^1 f_{n*} \mathbb{Q})). \end{aligned}$$

where q_{1*} is the trace morphism for the covering q_1 .

(ii) Similarly, $R_p = p^k I_p^*$.

□

The distrustful reader could forget the adelic preliminaries and define T_p by (i). When $n = 1$ or 2 , one puts ${}_n W = W^{K_n}$, so that

$${}_1 W = {}_n W^{\text{GL}_2(\mathbb{Z}/(n))}.$$

If S_{k+2} denotes the space of cusp forms, for the group $\text{SL}_2(\mathbb{Z})$, of weight $k + 2$, the Shimura isomorphism (3.11) induces an isomorphism

$${}_1^k W_\infty = {}_1^k W \otimes \mathbb{C} = S_{k+2} \oplus \bar{S}_{k+2}.$$

It is tiresome, but routine, to prove the following.

Proposition (3.19). The endomorphism T_p of ${}_1^k W_\infty$ is identified, via the Shimura isomorphism, with the direct sum of the Hecke operator on S_{k+2} , including the factor p^{k-1} , and its conjugate.

□

(3.20) One has canonically

$$\bigwedge^2 R^1 f_{n*} \mathbb{Z}_\ell \simeq R^2 f_{n*} \mathbb{Z}_\ell \simeq \mathbb{Z}_\ell(-1),$$

so that $\text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell)$ is equipped with a bilinear form, symmetric for k even and alternating for k odd, with values in $\mathbb{Z}_\ell(-k)$. The form induced by tensoring with $\mathbb{Q}_\ell$ is nondegenerate.

If F is an lcc $\mathbb{Q}_\ell$ -sheaf over a smooth scheme X of pure dimension n over an algebraically closed field k , then Poincaré duality gives

$$\begin{aligned} H^i(X, F)^\vee &\simeq H_c^{2n-i}(X, \text{Hom}(F, \mathbb{Q}_\ell(n))), \\ H_c^i(X, F)^\vee &\simeq H^{2n-i}(X, \text{Hom}(F, \mathbb{Q}_\ell(n))), \\ \tilde{H}^i(X, F)^\vee &\simeq \tilde{H}^{2n-i}(X, \text{Hom}(F, \mathbb{Q}_\ell(n))). \end{aligned}$$

Taking $X = \overline{M}_n$ and $F = \text{Sym}^k(R^1 f_{n*} \mathbb{Q}_\ell)$ in these considerations, one defines a nondegenerate bilinear form ${}_n(\cdot, \cdot)$ on ${}_n^k W_\ell$ with values in $\mathbb{Q}_\ell(-k-1)$. This form is symmetric for k odd and alternating for k even. This is the ℓ -adic analogue of the Petersson inner product. If $n \mid m$, and if the covering $\psi : M_m \rightarrow M_n$ is of degree d , then one has

$${}_m(\psi^* x, \psi^* y) = d \cdot {}_n(x, y).$$

Source note. The printed text spells the name “Peterson” here and again in the proof of (5.6), and “Perterson” at the end. The standard name “Petersson” is restored throughout. The same page’s evident spelling slip “isomprhism” is regularized to “isomorphism.”

4 The Congruence Formula

In this section we fix integers $k \geq 0$ and $n \geq 3$, and prime numbers p and ℓ . We suppose that p is prime to ℓ and n . We denote by $f_n : E \rightarrow M_n$ the universal elliptic curve over M_n , equipped with $\alpha : E_n \xrightarrow{\sim} \mathbb{Z}/(n)^2$.

Whatever the scheme Y , one denotes by a the unique morphism of Y to $\text{Spec}(\mathbb{Z})$ or, if necessary, to a subscheme of $\text{Spec}(\mathbb{Z})$. If Y is separated and of finite type over $\text{Spec}(\mathbb{Z})$, and if F is a $\mathbb{Z}_\ell$ - or $\mathbb{Q}_\ell$ -sheaf on Y , one denotes by $R^i a_*(Y, F)$, respectively $R^i a_!(Y, F)$, respectively $R^i \tilde{a}(Y, F)$, the $\mathbb{Z}_\ell$ - or $\mathbb{Q}_\ell$ -sheaf over $\text{Spec}(\mathbb{Z})$ that is the i th higher direct image of F under a , respectively the i th direct image with proper supports, respectively $\text{Im}(R^i a_!(Y, F) \rightarrow R^i a_*(Y, F))$. For $m \in \mathbb{N}$, one puts

$$Y[1/m] = Y \times \text{Spec}(\mathbb{Z}[1/m]).$$

Theorem (4.1, Igusa [1]). *The scheme M_n can be compactified to a scheme of curves M_n^* that is projective and smooth over $\text{Spec}(\mathbb{Z}[1/n])$, such that $M_n^* \setminus M_n$ is an étale covering of $\text{Spec}(\mathbb{Z}[1/n])$.*

The schemes M_n are formally smooth, thus smooth over $\text{Spec}(\mathbb{Z})$. The modular invariant j of the universal curve over M_n is a morphism of M_n to the affine line $\mathbb{A}^1$ over $\text{Spec}(\mathbb{Z}[1/n])$. The morphism j is finite, and is an étale covering away from the sections 0 and 1728 of $\mathbb{A}^1$; in fact:

- (a) Two elliptic curves over an algebraically closed field with the same j -invariant are isomorphic (e.g. [8] 6.3), thus the geometric fibers of j are finite. The schemes M_n and $\mathbb{A}^1$ being smooth of the same dimension over $\text{Spec}(\mathbb{Z})$, j is quasi-finite and flat.
- (b) If E is an elliptic curve over the field of fractions K of a discrete valuation ring R , of j -invariant in R , and whose points of order n are rational over K , then E has good reduction. The valuative criterion for properness shows thus that j is proper.
- (c) If E and F are two elliptic curves over a scheme S , of the same j -invariant, and if j and $j - 1728$ are invertible, then the scheme $\text{Isom}(S; E, F)$ of isomorphisms between E and F is étale over S ([8] 6.3). In the diagram

$$\begin{array}{ccc} \text{Isom}(M_n \times_{\mathbb{A}^1} M_n; \text{pr}_1^* E, \text{pr}_2^* E) & \sim & M_n \times \text{GL}_2(\mathbb{Z}/(n)) \\ \downarrow u & & \downarrow v \\ M_n \times_{\mathbb{A}^1} M_n & \xrightarrow{\text{pr}_1} & M_n, \end{array}$$

where $j \neq 0, 1728$, u and v are étale surjective, thus pr_1 is étale and, by flat descent, j is étale.

The section at infinity of the projective line $\mathbb{P}^1 \supset \mathbb{A}^1$ over $\text{Spec}(\mathbb{Z}[1/n])$ is a regular divisor whose generic point is of characteristic 0 in a regular scheme. It follows from a theorem of Abhyankar (see [5]) that along this divisor $j = \infty$, M_n is tamely ramified over $\mathbb{P}^1$, and that the normalization M_n^* of $\mathbb{P}^1$ in M_n satisfies (4.1). $\square$

Source note. The English retype's "The schemes M_n is" is regularized to "are." Both printed witnesses spell Abhyankar's name "Abyankhar," and the English retype renders the standard French term *modérément ramifié* as the unresolved "moderately (tamely?) ramified." The standard name and English term "tamely ramified" are delivered above.

It follows from the same theorem that the lcc $\mathbb{Z}_\ell$ -sheaves $R^i f_{n*} \mathbb{Z}_\ell$ on $M_n[1/\ell]$ are tamely ramified at infinity. Hence, from (4.1) and the specialization theorems for ℓ -adic cohomology (see [5]), it follows that $R^i a_*(M_n, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell))$, $R^i a_!(M_n, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell))$, and therefore $R^i \tilde{a}(M_n, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell))$ are lcc $\mathbb{Z}_\ell$ -sheaves over $\text{Spec}(\mathbb{Z}[1/n, 1/\ell])$, whose formation is compatible with all base changes.

Corollary (4.2). *The Galois module ${}_n W_\ell$ is the fiber of the lcc $\mathbb{Q}_\ell$ -sheaf*

$$R^1 \tilde{a}(M_n, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell)) \otimes \mathbb{Q}_\ell$$

over $\text{Spec}(\mathbb{Z}[1/n, 1/\ell])$ at the geometric point $\overline{\mathbb{Q}}$. It is unramified away from n and ℓ .

$\square$

Let the two commutative diagrams over $M_n \otimes \mathbb{F}_p$

$$\begin{array}{ccc} & \mathbb{Z}/(n)^2 & \\ \alpha \nearrow & & \nwarrow \alpha^{(p)} \\ E_n & \xrightarrow{\quad} & E_n^{(p)} \\ \downarrow & & \downarrow \\ E & \xrightarrow{F} & E^{(p)} \end{array} \quad \begin{array}{ccc} & \mathbb{Z}/(n)^2 & \\ p\alpha^{(p)} \nearrow & & \nwarrow \alpha \\ E_n^{(p)} & \xrightarrow{\quad} & E_n \\ \downarrow & & \downarrow \\ E^{(p)} & \xrightarrow{V} & E \end{array}$$

be written more briefly

$$F : (E, \alpha) \rightarrow (E^{(p)}, \alpha^{(p)}) \quad \text{and} \quad V : (E^{(p)}, p\alpha^{(p)}) \rightarrow (E, \alpha),$$

where F is the Frobenius morphism and V , its transpose, is the Verschiebung. These diagrams define morphisms Φ_1 and Φ_2 of $M_n \otimes \mathbb{F}_p$ to $M_{n,p}$. These morphisms are finite, considered as sections of q_1 and q_2 , and define a morphism

$$\Phi = \Phi_1 \coprod \Phi_2 : M_n \otimes \mathbb{F}_p \coprod M_n \otimes \mathbb{F}_p \rightarrow M_{n,p} \otimes \mathbb{F}_p.$$

Source note. The inherited arrays incorrectly repeated the labels F and V on the induced arrows between the n -torsion subgroup schemes. In the source those upper horizontal arrows are unlabeled; only the maps between the elliptic curves carry F and V . The native diagrams above restore that distinction. Let Φ^h be the restriction of Φ to the opens M_n^h and $M_{n,p}^h$ of $M_n \otimes \mathbb{F}_p$ and $M_{n,p} \otimes \mathbb{F}_p$ corresponding to curves of nonzero Hasse invariant h .

Proposition (4.3). Φ^h is an isomorphism.

Let $\varphi : E_1 \rightarrow E_2$ be a p -isogeny between elliptic curves of invertible Hasse invariant over a scheme S of characteristic p . At each geometric point of S , either the kernel $\ker(\varphi)$ of φ is étale over S , or its Cartier dual, isomorphic to $\ker({}^t\varphi)$, is étale over S . The property “ $\ker(\varphi)$ is étale” is an open property, so that locally on S , either $\ker(\varphi)$ is purely infinitesimal, or $\ker({}^t\varphi)$ is. The only infinitesimal subgroup of order p of E_1 or E_2 being the kernel of Frobenius, in the first case φ is isomorphic to $F : E_1 \rightarrow E_1^{(p)}$, and in the second case ${}^t\varphi$ is isomorphic to $F : E_2 \rightarrow E_2^{(p)}$ and φ to $V : E_2^{(p)} \rightarrow E_2$. $\square$

Proposition (4.4).

- (i) The scheme $M_{n,p}$ is smooth over $\text{Spec}(\mathbb{Z})$ away from points of characteristic p where $h = 0$.
- (ii) The morphisms q_1 and q_2 induce finite flat morphisms q'_1 and q'_2 from the normalization $M'_{n,p}$ of $M_{n,p}$ to M_n .
- (iii) The morphism Φ can be factored through a surjective morphism

$$\Phi' : M_n \otimes \mathbb{F}_p \coprod M_n \otimes \mathbb{F}_p \rightarrow M'_{n,p} \otimes \mathbb{F}_p.$$

The automorphism σ of (3.15) exchanges φ and ${}^t\varphi$, so that it suffices to prove (i) at the points of characteristic p of $M_{n,p}$ where the kernel of φ is infinitesimal: there is no obstruction to infinitesimally lifting an elliptic curve and the infinitesimal part of the kernel of multiplication by p .

Where $p = h = 0$, the fiber of the finite morphism (3.15) $q_i : M_{n,p} \rightarrow M_n$ is reduced to a point, so that the open of smoothness of $M_{n,p}$ is dense in $M_{n,p}$ and $M'_{n,p}$ is everywhere of dimension 2. The scheme M_n being regular, following EGA 0_{IV} 16.5.1 and 17.3.5(ii), the morphism $q_i : M'_{n,p} \rightarrow M_n$ is flat. Finally, (iii) results from the fact that Φ is finite and $M_n \otimes \mathbb{F}_p$ is a normal curve. $\square$

The Hecke endomorphism T_p of ${}_nW_\ell$, such as is made explicit in (3.18), is the tensorization with $\mathbb{Q}_\ell$ of the fiber at the geometric point $\bar{\mathbb{Q}}$ of $\text{Spec}(\mathbb{Z}[1/n, 1/\ell])$ of the endomorphism, again denoted by T_p , of $R^1\tilde{a}(M_n, \text{Sym}^k(R^1f_{n*}\mathbb{Z}_\ell))$ defined by the correspondence

$$\begin{array}{ccccc}
 & q_1'^* E & \xrightarrow{\varphi} & q_2'^* E & \\
 & \swarrow & & \searrow & \\
 E & & & & E \\
 & \searrow & & \swarrow & \\
 & M'_{n,p} & & & \\
 & \swarrow & & \searrow & \\
 f_n \swarrow & & & & \searrow f_n \\
 & M_n & & & M_n \\
 & \nwarrow q'_1 & & \nearrow q'_2 & \\
 & & & &
 \end{array} \tag{4.5}$$

with

$$T_p = q_{1*}' \varphi^* q_2'^* \quad (\text{cf. 3.18}).$$

Source note. As in the inherited version of (3.16), the inherited array for (4.5) attached u and v to the lower moduli object and collapsed two distinct pullback-to-curve maps. The native diagram restores the source’s full nine-arrow topology. The endomorphisms R_p and I_p can be interpreted in the same way.

Lemma (4.6). *Let X, Y, Z_1 , and Z_2 be four schemes that are separated and of finite type over a noetherian scheme S , let F be a $\mathbb{Z}_\ell$ -sheaf on X , let G be a $\mathbb{Z}_\ell$ -sheaf on Y , and denote by a each of the structural maps from X, Y, Z_1 or Z_2 to S . Suppose we have the following commutative diagram of S -schemes and morphisms of sheaves:*

$$\begin{array}{ccc}
 y_1^* G & \xrightarrow{z_1} & x_1^* F \\
 & & \\
 & \begin{array}{ccc} & Z_1 & \xrightarrow{f} & Z_2 \\ & \swarrow x_1 & \searrow x_2 & \swarrow y_1 & \searrow y_2 \\ X & & & & Y \end{array} &
 \end{array}$$

Suppose that $f^ z_2 = z_1$, that y_1 and y_2 are proper, that x_1 and x_2 are finite and flat, and that, for every geometric point s of Z_2 , the multiplicity of s in its fiber $x_2^{-1}(x_2(s))$ is equal to the sum of the multiplicities in their fibers, for x_1 , of the geometric points of Z_1 in the inverse image of s under f . Then the diagram*

$$\begin{array}{ccccccc}
 R^i \tilde{a}(Y, G) & \xrightarrow{y_1^*} & R^i \tilde{a}(Z_1, G) & \xrightarrow{z_1} & R^i \tilde{a}(Z_1, F) & \xrightarrow{x_{1*}} & R^i \tilde{a}(X, F) \\
 \parallel & & \uparrow f^* & & \uparrow f^* & & \parallel \\
 R^i \tilde{a}(Y, G) & \xrightarrow{y_2^*} & R^i \tilde{a}(Z_2, G) & \xrightarrow{z_2} & R^i \tilde{a}(Z_2, F) & \xrightarrow{x_{2*}} & R^i \tilde{a}(X, F)
 \end{array}$$

commutes.

Source note. The inherited arrays lost the shared $Z_1 \rightarrow Z_2$ object pair in the structural diagram and misaligned the vertical maps in the two cohomological diagrams. The diagrams are rebuilt natively with the source's shared objects and its distinct diagonal, vertical, equality, pullback, and trace arrows. An earlier repair duplicated $Z_1 \rightarrow Z_2$ into two disconnected copies; direct replay of the French original at printed p. 164 exposed that remaining topology error, which is now repaired in both editions.

This lemma results from the analogous lemmas for $R^i a_!$ and $R^i a_*$. The commutativity of the first squares is trivial. The last is rewritten

$$\begin{array}{ccccc}
 R^i \tilde{a}(Z_1, x_1^* F) & \xleftarrow{\sim} & R^i \tilde{a}(X, x_{1*} x_1^* F) & \xrightarrow{\text{Tr}} & R^i \tilde{a}(X, F) \\
 \uparrow & & \uparrow & & \parallel \\
 R^i \tilde{a}(Z_2, x_2^* F) & \xleftarrow{\sim} & R^i \tilde{a}(X, x_{2*} x_2^* F) & \xrightarrow{\text{Tr}} & R^i \tilde{a}(X, F)
 \end{array}$$

and one recalls the definition of the trace in verifying that the square

$$\begin{array}{ccc}
 x_{1*} x_1^* F & \xrightarrow{\text{Tr}} & F \\
 \uparrow & & \parallel \\
 x_{2*} x_2^* F & \xrightarrow{\text{Tr}} & F
 \end{array}$$

is commutative. □

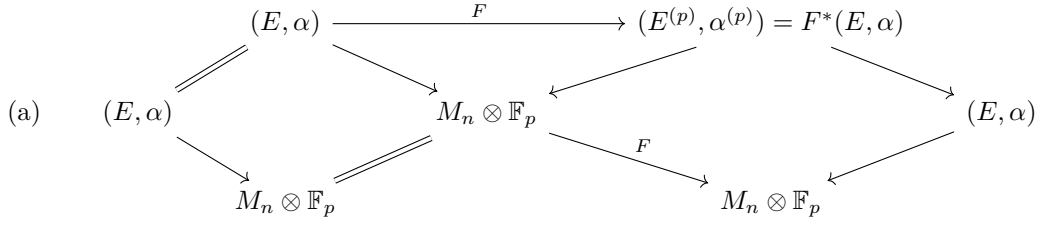
(4.7) One denotes by $T_p/\mathbb{F}_p$ the endomorphism induced by T_p on the restriction to $\text{Spec}(\mathbb{F}_p)$ of the lcc $\mathbb{Z}_\ell$ -sheaf $R^1 \tilde{a}(M_n, \text{Sym}^k R^1 f_{n*} \mathbb{Z}_\ell)$. One has

$$R^1 \tilde{a}(M_n, \text{Sym}^k R^1 f_{n*} \mathbb{Z}_\ell)|_{\text{Spec}(\mathbb{F}_p)} \xrightarrow{\sim} R^1 \tilde{a}(M_n \otimes \mathbb{F}_p, \text{Sym}^k R^1 f_{n*} \mathbb{Z}_\ell);$$

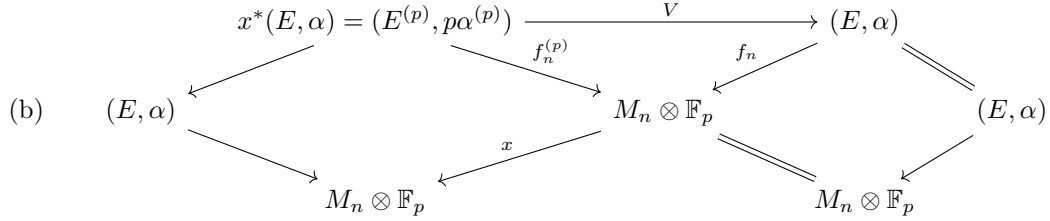
the formation of the trace morphism for a finite flat morphism is compatible with change of base, so that $T_p/\mathbb{F}_p$ can be constructed, over the model (3.18), starting from the fiber over $\mathbb{F}_p$ of the “correspondence” (4.5). Lemma (4.6), applied to the commutative diagrams

$$\begin{array}{ccc}
 M_n \otimes \mathbb{F}_p \amalg M_n \otimes \mathbb{F}_p & \xrightarrow{\Phi'} & M'_{n,p} \otimes \mathbb{F}_p \\
 \downarrow & \swarrow q'_1 & \\
 M_n \otimes \mathbb{F}_p & &
 \end{array}
 \quad
 \begin{array}{ccc}
 M_n \otimes \mathbb{F}_p \amalg M_n \otimes \mathbb{F}_p & \xrightarrow{\Phi'} & M'_{n,p} \otimes \mathbb{F}_p \\
 & \searrow q'_2 & \downarrow \\
 & & M_n \otimes \mathbb{F}_p,
 \end{array}$$

furnishes then a decomposition of $T_p/\mathbb{F}_p$ into the sum of endomorphisms defined by the two following correspondences:



where F is the absolute Frobenius. One recognizes in this correspondence the geometric Frobenius



Source note. The inherited arrays for correspondences (a) and (b) retained only four of the eight descending source relations and rendered two equality relations as arrows. The native diagrams restore every diagonal, both equality relations in each correspondence, and the labels $f_n^{(p)}$, f_n , x , and F at their printed attachment sites. The map x is the composite map $I_p^{-1} \circ F$:

$$\begin{array}{ccccc}
 (E, \alpha) & \longleftarrow & (E, p\alpha) & \longleftarrow & (E^{(p)}, p\alpha^{(p)}) \\
 \downarrow & & \downarrow & & \downarrow \\
 M_n \otimes \mathbb{F}_p & \xleftarrow{I_p^{-1}} & M_n \otimes \mathbb{F}_p & \xleftarrow{F} & M_n \otimes \mathbb{F}_p.
 \end{array}$$

The corresponding endomorphism is thus the composite of

$$V : R^1\tilde{a}(M_n \otimes \mathbb{F}_p, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell)) \xrightarrow{V^*} R^1\tilde{a}(M_n \otimes \mathbb{F}_p, \text{Sym}^k(R^1 f_{n*}^{(p)} \mathbb{Z}_\ell)) \xrightarrow{\text{Tr}_F} R^1\tilde{a}(M_n \otimes \mathbb{F}_p, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell))$$

and of

$$I_p^* = \text{Tr}_{I_p^{-1}} : \text{endomorphism of } R^1\tilde{a}(M_n \otimes \mathbb{F}_p, \text{Sym}^k R^1 f_{n*} \mathbb{Z}_\ell).$$

Proposition (4.8). *One has $T_p/\mathbb{F}_p = F + I_p^* V$, and:*

- (i) *F can be identified with the inverse of the “arithmetic” Frobenius element φ_p of the Galois group $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ acting on $\tilde{H}^1(M_n \otimes \overline{\mathbb{F}}_p, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell))$;*
- (ii) *F and V are transposes of one another, relative to the scalar product (3.20);*
- (iii) *$FV = VF = p^{k+1}$.*

For the relation (i) between the geometric and arithmetic Frobenius, one is referred to the exposé of C. Houzel (SGA 5.XV). The composite VF is the composite of the homomorphisms obtained from the following maps:

$$\begin{array}{ccccccc}
 E & \longleftarrow & E^{(p)} & \xrightarrow{F_E} & E & \xrightarrow{V_E} & E^{(p)} \longrightarrow E \\
 \downarrow & & \searrow & & \downarrow & \swarrow & \\
 M_n & \xrightarrow{F} & M_n & & M_n & \xrightarrow{F} & M_n
 \end{array}$$

Source note. The inherited array collapsed the printed five-object $E \leftarrow E^{(p)} \rightarrow E \rightarrow E^{(p)} \rightarrow E$ diagram to three objects and thereby omitted both intermediate Frobenius twists and their diagonal structure maps. The complete native diagram above restores all five objects and all eleven source arrows. Thus

$$VF = \text{Tr}_F \circ F_E^* \circ V_E^* \circ F^*.$$

The map $F_E^* V_E^* = (F_E V_E)^* = (p \cdot 1_E)^*$ acts by multiplication by p^k on $\mathrm{Sym}^k R^1 f_{n*} \mathbb{Z}_\ell$, so that

$$VF = p^k \mathrm{Tr}_F \circ F^* = p^k \cdot p = p^{k+1},$$

because $F : M_n \rightarrow M_n$ is of degree p .

By transport of structure, φ_p respects the scalar product (3.20) with values in $\mathbb{Q}_\ell(-k-1)$, a group on which φ_p acts by multiplication by p^{-k-1} . One has thus

$$(Fx, y) = p^{k+1}(\varphi_p Fx, \varphi_p y) = (x, p^{k+1} F^{-1} y) = (x, Vy).$$

□

The following theorem, synonymous with (4.8), goes back to Eichler.

Theorem (4.9, The Congruence Formula). *Let $K_{n,\ell}$ be the largest subextension of $\overline{\mathbb{Q}}$ that is unramified away from n and ℓ , let φ_p be a Frobenius element relative to p in $\mathrm{Gal}(K_{n,\ell}/\mathbb{Q})$, let F be the endomorphism φ_p^{-1} of ${}_n W_\ell$, and let V be the transpose of F relative to the scalar product (3.20). Then*

$$T_p = F + I_p^* V, \quad FV = p^{k+1}, \quad 1 - T_p X + p R_p X^2 = (1 - FX)(1 - I_p^* V X).$$

□

5 Weil implies Ramanujan

If p is a prime number and X a scheme over $\mathbb{F}_p$, then one denotes by $\overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$, by $F : X \rightarrow X$ the “geometric” Frobenius endomorphism, and one puts $\overline{X} = X \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$; ℓ always denotes a prime number different from p .

By the “Weil conjectures” one means to claim the following: let X be a projective smooth scheme over $\mathbb{F}_p$ and let ℓ be a prime number different from p . Then the eigenvalues of the endomorphism F^* of $H^i(\overline{X}, \mathbb{Q}_\ell)$ are algebraic integers all of whose complex conjugates have absolute value $p^{i/2}$.

With the hypotheses and notations of (4.9), one has, recalling that $(p, n) = 1$:

Theorem (5.1). *If the Weil conjectures are true, then the eigenvalues of the endomorphism F of ${}_n^k W_\ell$ are algebraic integers, all of whose complex conjugates have absolute value $p^{(k+1)/2}$.*

Source note. The printed statement says “the absolute values of the endomorphism” and prints $p^{k+1/2}$. The theorem concerns the eigenvalues of F , and the weight is $k+1$; the mathematically required reading $p^{(k+1)/2}$ is delivered above.

Assume the Weil conjectures.

Lemma (5.2, modulo Weil). *Let X be a smooth scheme over $\mathbb{F}_p$, which can be represented as an open in a smooth projective scheme X^* . Then the eigenvalues of the endomorphism F^* of $\tilde{H}^i(X, \mathbb{Q}_\ell)$ are algebraic integers of absolute value $p^{i/2}$.*

Source note. The printed phrase “the absolute values of [the] endomorphism” is corrected to “the eigenvalues of the endomorphism”; the displayed absolute value $p^{i/2}$ is unchanged.

The natural map of $H_c^i(X, \mathbb{Q}_\ell)$ to $H^i(X, \mathbb{Q}_\ell)$ can be factored through $H^i(X^*, \mathbb{Q}_\ell)$:

$$H_c^i(X, \mathbb{Q}_\ell) \rightarrow H^i(X^*, \mathbb{Q}_\ell) \rightarrow H^i(X, \mathbb{Q}_\ell),$$

so that, as a $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ -module, $\tilde{H}^i(X, \mathbb{Q}_\ell)$ is the quotient of a subobject of $H^i(X^*, \mathbb{Q}_\ell)$. □

Lemma (5.3, modulo Weil). *Let S be a smooth scheme over $\mathbb{F}_p$ and $f : A \rightarrow S$ an abelian scheme over S . Suppose that A can be represented as an open in a projective smooth scheme A^* over $\mathbb{F}_p$. Then the geometric Frobenius F^* of $\tilde{H}^i(S, R^j f_* \mathbb{Q}_\ell)$ has eigenvalues that are algebraic integers of absolute value $p^{(i+j)/2}$.*

Source note. The printed exponent is $i + j/2$. Since the cohomological weight is $i + j$, the required exponent is $(i + j)/2$, as delivered above and used in the proof via (5.2).

Let m be an integer > 1 , and consider the Leray spectral sequences

$$E : E_2^{ij} = H^i(\bar{S}, R^j f_* \mathbb{Q}_\ell) \implies H^{i+j}(\bar{A}, \mathbb{Q}_\ell), \quad {}_c E : {}_c E_2^{ij} = H_c^i(\bar{S}, R^j f_* \mathbb{Q}_\ell) \implies H_c^{i+j}(\bar{A}, \mathbb{Q}_\ell).$$

The endomorphism of multiplication by m , $\psi_m = m \cdot 1_A$, defines endomorphisms of E and ${}_c E$ that fit into a commutative diagram

$$\begin{array}{ccc} {}_c E & \longrightarrow & E \\ \psi_m^* \downarrow & & \psi_m^* \downarrow \\ {}_c E & \longrightarrow & E. \end{array}$$

ψ_m^* acts on $R^j f_* \mathbb{Q}_\ell$ by multiplication by m^j , so that ψ_m^* acts by multiplication by m^j on the terms ${}_c E_r^{ij}$ and E_r^{ij} of ${}_c E$ and E . The maps d_r for $r \geq 2$ commute with ψ_m^* , and send E_r^{ij} , respectively ${}_c E_r^{ij}$, to $E_r^{i'j'}$, respectively ${}_c E_r^{i'j'}$, with $j \neq j'$. These maps are zero, and E_2^{ij} , respectively ${}_c E_2^{ij}$, can be identified with a subspace of $H^{i+j}(\bar{A}, \mathbb{Q}_\ell)$, respectively $H_c^{i+j}(\bar{A}, \mathbb{Q}_\ell)$, where $\psi_m^* = m^j$. Consequently, $\tilde{H}^i(S, R^j f_* \mathbb{Q}_\ell)$ is identified, as a Galois module, with a subspace of $\tilde{H}^{i+j}(A, \mathbb{Q}_\ell)$ where $\psi_m^* = m^j$, and one applies (5.2). The trick used here is due to Lieberman. $\square$

Source note. The printed proof says that the differentials are nonzero. Since they commute with ψ_m^* but go between the distinct eigenspaces m^j and $m^{j'}$ with $j \neq j'$, they are zero; this is precisely the degeneration used in the following identification.

Let $f_n : E \rightarrow M_n \otimes \mathbb{F}_p$ be the universal elliptic curve over $M_n \otimes \mathbb{F}_p$, and let $f_{n,k} : E_k \rightarrow M_n \otimes \mathbb{F}_p$ be its k -fold fiber product with itself. The Künneth formula shows that the $\mathbb{Q}_\ell$ -sheaf $R^k f_{n,k*} \mathbb{Q}_\ell$ admits as a direct factor the k -fold tensor power of $R^1 f_{n*} \mathbb{Q}_\ell$; the latter in turn contains as a direct factor the $\mathbb{Q}_\ell$ -sheaf $\text{Sym}^k(R^1 f_{n*} \mathbb{Q}_\ell)$. Theorem 5.1 results thus from (5.3) and the following lemma.

Lemma (5.4). *The scheme E_k is an open in a smooth projective scheme E_k^* over $\mathbb{F}_p$.*

Let E^* be the Néron minimal model of E over $M_n^* \otimes \mathbb{F}_p$ (4.1). The scheme E^* is smooth and projective over $\mathbb{F}_p$. Since $n \geq 3$ and the points of order n of E form a trivial covering of $M_n \otimes \mathbb{F}_p$, the Néron model is “semistable,” case a or b_m in Néron’s classification. In particular, the projection $f_n : E^* \rightarrow M_n^*$ has only a finite number of nonsmooth points, and at these points f_n is nondegenerate, presenting an ordinary quadratic singularity.

Let E_k^{**} be the k -fold fiber product of E^* over M_n^* . To prove (5.4), it suffices to resolve the singularities of E_k^{**} without touching the open E_k . We first prove:

Lemma (5.5). *Let V be the subvariety of affine space over a field k , with coordinates $(X_i)_{0 \leq i \leq r}$, $(Y_i)_{0 \leq i \leq r}$, and $(T_i)_{1 \leq i \leq s}$, with equation*

$$X_0 Y_0 = X_1 Y_1 = \cdots = X_r Y_r.$$

Let $\mathfrak{m}$ be the ideal of $\mathcal{O}_V$ generated by the monomials obtained from the monomial $\prod_{i=0}^r X_i^i$ by a permutation of the coordinates which respects the set of pairs $\{X_i, Y_i\}$, $0 \leq i \leq r$. Then $\mathfrak{m} = \mathcal{O}_V$ away from the singular locus of V , and the variety $\tilde{V}$ obtained from V by blowing up $\mathfrak{m}$ is smooth over k .

The singular locus is the place where the four coordinates X_i, Y_i, X_j, Y_j for $i \neq j$ vanish. The open affine of $\tilde{V}$ defined by the element $\prod_{i=0}^r X_i^i$ of the ideal $\mathfrak{m}$ of blowing up is the spectrum of the regular ring

$$k[Y_0/X_1, X_0/X_1, X_1/X_2, \dots, X_{r-1}/X_r, X_r, T_1, \dots, T_s]$$

(for the proof, note that $X_i/X_{i+1} = Y_{i+1}/Y_i$), and 5.5 results. $\square$

One still shows that, locally for the étale topology, the singularities of E_k^{**} are isomorphic to those of V for $r = k - 1$, and that this allows the definition on E_k^{**} of an ideal $\mathfrak{m}$ analogous to the ideal $\mathfrak{m}$ of (5.5). Blowing up this ideal, one obtains E_k^* . $\square$

An approximation to the following theorem has been proven by Ihara [2].

Theorem (5.6). *The Weil conjectures imply the Ramanujan conjecture.*

We note first that (5.1) is true for $n = 1$, because ${}_1^k W_\ell$ is the Galois submodule of ${}_m^k W_\ell$ invariant under $\text{GL}_2(\mathbb{Z}/(m))$. On ${}_1^k W_\ell$, I_p^* induces the identity, and (4.8) reduces to

$$1 - T_p X + p^{k+1} X^2 = (1 - FX)(1 - VX).$$

The endomorphisms F and V are transposes of each other, so that

$$\det(1 - FX; {}_1^k W_\ell) = \det(1 - VX; {}_1^k W_\ell).$$

The action of T_p on ${}^k_1W_\ell$ is induced by its action on k_1W , and is compatible with the decomposition of ${}^k_1W \otimes \mathbb{C}$ into the sum of the space S_{k+2} of cusp forms relative to $\mathrm{SL}_2(\mathbb{Z})$ of weight $k+2$, and of the complex conjugate space. From the Hermitian property for T_p , for the Petersson inner product, and from (3.19), one deduces then that

$$\det(1 - T_p X + p^{k+1} X^2; {}^k_1W_\ell) = \det(1 - T_p X + p^{k+1} X^2; S_{k+2})^2,$$

and

$$\det(1 - T_p X + p^{k+1} X^2; S_{k+2})^2 = \det(1 - F X; {}^k_1W_\ell)^2,$$

so that

$$\det(1 - T_p X + p^{k+1} X^2; S_{k+2}) = \det(1 - F X; {}^k_1W_\ell). \quad (5.7)$$

Resume the notations of section 1 and make $k = 10$. By virtue of Hecke's theory and of (3.19), (5.7) can be rewritten

$$H_p(X) = \det(1 - F X; {}^{10}_1W_\ell),$$

and one applies (5.1). □

One verifies in the same way that the Weil conjectures imply Petersson's generalization of the Ramanujan conjecture.

References

- [1] J. Igusa, *Kroneckerian model of fields of elliptic modular functions*, Am. J. of Math. **81** (1959), 561–577.
- [2] Y. Ihara, *Hecke polynomials as congruence zeta functions in elliptic modular case*, Ann. of Math., S.2 **85** (1967), 267–295.
- [3] J.-P. Jouanolou, Exposés V and VI of SGA 5.
- [4] M. Kuga and G. Shimura, *On the zeta function of a fibre variety whose fibres are abelian varieties*, Ann. of Math., S.2 **82** (1965), 478–539.
- [5] M. Raynaud, Exposé XIII of SGA 1 and appendix (to appear).
- [6] J.-P. Serre, *Une interprétation des congruences relatives à la fonction τ de Ramanujan*, Sémin. Delange–Pisot–Poitou, 1967/68, no. 14.
- [7] G. Shimura, *Sur les intégrales attachées aux formes automorphes*, J. Math. Soc. of Japan **11** (1959), 291–311.
- [8] J. Tate, *Courbes elliptiques: formulaire*, mis au goût du jour par P. Deligne, mimeographed notes by I.H.E.S.
- [9] J.-L. Verdier, *Sur les intégrales attachées aux formes automorphes* (d'après G. Shimura), Sémin. Bourbaki, Février 1961, exp. 216.

Initials. EGA: *Éléments de géométrie algébrique*, by A. Grothendieck and J. Dieudonné, Publ. Math. I.H.E.S.
SGA: *Séminaire de géométrie algébrique du Bois-Marie*, mimeographed notes by I.H.E.S., to appear from North-Holland.